

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-064490

(43)Date of publication of application : 26.02.2004

(51)Int.Cl. H04L 29/06
G06F 13/00
H04L 12/66

(21)Application number : 2002-221055

(71)Applicant : FUJITSU LTD

(22)Date of filing : 30.07.2002

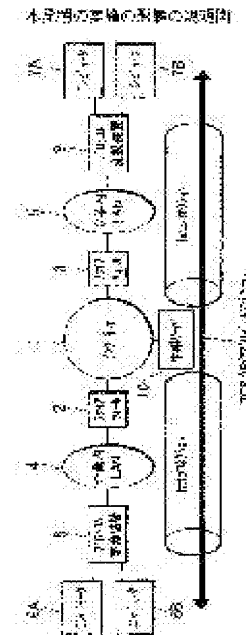
(72)Inventor : IKEDA MITSUTOSHI
HAYASHIDA TAKASHI
KAIZUKA TOMONORI
SHIMOYAMA MOTOAKI
SATO HIROKO

(54) DATA COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To enable data communication without being conscious of being connected to the Internet via a firewall, in a data communication system for performing the data communication among communication devices via the Internet.

SOLUTION: The data communication system for performing the data communication among the communication devices including computers 6A, 6B, 7A, 7B and intracorporate LANs 4, 5, etc., connected, respectively, to the Internet 1 via firewalls 2, 3, comprises protocol conversion devices 8, 9 for converting data from the communication devices of transmitting origins into packets in formats capable of passing through the firewalls 2, 3 to transmit them, and for recovering the packets received via the firewalls 2, 3 to data for communication devices of transmitting destinations between the communication devices and the firewalls 2, 3, and a relay server 10 for relaying/transmitting transmitting packets between the conversion devices 8, 9 to the Internet 1.



LEGAL STATUS

[Date of request for examination] 12.05.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-64490

(P2004-64490A)

(43) 公開日 平成16年2月26日(2004. 2. 26)

(51) Int. Cl.⁷

F I

テーマコード (参考)

H O 4 L 29/06

H O 4 L 13/00

3 O 5 B

5 B O 8 9

G O 6 F 13/00

G O 6 F 13/00

3 5 1 Z

5 K O 3 O

H O 4 L 12/66

H O 4 L 12/66

B

5 K O 3 4

審査請求 未請求 請求項の数 5 O L (全 15 頁)

(21) 出願番号 特願2002-221055 (P2002-221055)
 (22) 出願日 平成14年7月30日 (2002. 7. 30)

(71) 出願人 000005223
 富士通株式会社
 神奈川県川崎市中原区上小田中4丁目1番
 1号
 (74) 代理人 100105337
 弁理士 眞鍋 深
 (74) 代理人 100072833
 弁理士 柏谷 昭司
 (74) 代理人 100075890
 弁理士 渡邊 弘一
 (74) 代理人 100110238
 弁理士 伊藤 壽郎
 (72) 発明者 池田 充利
 神奈川県川崎市中原区上小田中4丁目1番
 1号 富士通株式会社内

最終頁に続く

(54) 【発明の名称】 データ通信システム

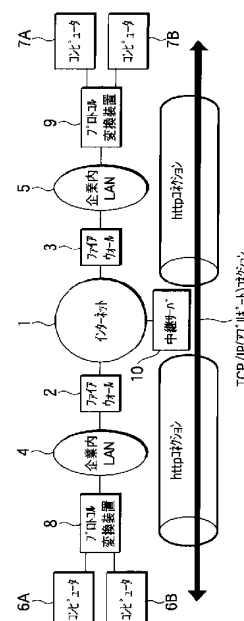
(57) 【要約】

【課題】 インターネットを介して通信装置間でデータ通信を行うデータ通信システムに関し、ファイアウォールを介してインターネットに接続されていることを意識することなく、データ信号を可能とする。

【解決手段】 ファイアウォール 2、3 を介してインターネット 1 にそれぞれ接続したコンピュータ 6 A、6 B、7 A、7 B や企業内 LAN 4、5 等を含む通信装置間でデータ通信を行うデータ通信システムであって、通信装置とファイアウォール 2、3 との間に、送信元の通信装置からのデータを、ファイアウォール 2、3 を透過可能な形式の packets に変換して送出し、ファイアウォール 2、3 を介して受信した packets を送信先の通信装置へのデータに復元するプロトコル変換装置 8、9 を設け、インターネット 1 に、プロトコル変換装置 8、9 間の伝送 packets を中継伝送する中継サーバ 10 を設けた構成とする。

【選択図】 図 1

本発明の実施の形態の説明図



【特許請求の範囲】

【請求項1】

ファイアウォールを介してインターネットにそれぞれ接続した通信装置間でデータ通信を行うデータ通信システムに於いて、

前記通信装置と前記ファイアウォールとの間に、送信元の通信装置からのデータを前記ファイアウォールを透過可能な形式の packets に変換して送出し、前記ファイアウォールを介して受信した前記 packets を送信先の通信装置へのデータに復元するプロトコル変換装置を設け、

送信元の通信装置を接続したプロトコル変換装置と送信先の通信装置を接続したプロトコル変換装置との間を前記ファイアウォールと前記インターネットとを介して中継接続する中継サーバを設けた

ことを特徴とするデータ通信システム。

【請求項2】

前記プロトコル変換装置は、送信先の通信装置のアドレスと前記中継サーバのアドレスとを対応させたルーティングテーブルと、送信元の通信装置からのデータを前記ファイアウォールを透過可能な形式の packets にラッピングするプロトコル変換部と、該プロトコル変換部により変換した packets を一時格納する送信バッファと、前記中継サーバとの間の接続要求及び前記送信バッファから読出した packets を前記中継サーバに送出する送信部と、前記中継サーバから中継送出された packets を受信する受信部と、該受信部により受信した packets を送信先の通信装置に送出するデータに変換するプロトコル変換部とを備えたことを特徴とする請求項1記載のデータ通信システム。

【請求項3】

前記中継サーバは、前記インターネットを介して前記プロトコル変換装置との間のコネクションを形成して、送信元側の前記プロトコル変換装置により変換した packets を受信する処理部と、該処理部により受信した packets を一時格納する送信バッファと、該送信バッファから packets を読出して送信先側の前記プロトコル変換装置へ送信する処理部とを含む構成を有することを特徴とする請求項1記載のデータ通信システム。

【請求項4】

前記プロトコル変換装置及び前記中継サーバは、相互間で伝送する packets に通番を付加して送信し、該 packets を受信して前記通番を抽出し、該通番を付加した応答を送信する構成を備えたことを特徴とする請求項1乃至3の何れか1項記載のデータ通信システム。

【請求項5】

前記中継サーバは、前記プロトコル変換装置を登録する登録手段と、該登録手段に登録されたプロトコル変換装置間のみ前記ファイアウォールを透過可能な形式の packets の中継送出を行う構成を備えたことを特徴とする請求項1乃至4の何れか1項記載のデータ通信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、コンピュータ等を含む通信装置をインターネットにファイアウォールを介して接続し、インターネットを介して通信装置間でデータ通信を行うデータ通信システムに関する。

【0002】

【従来の技術】

複数のコンピュータを接続した LAN (Local Area Network; ローカル・エリア・ネットワーク) 間を専用線で接続した企業内等のデータ通信システムが知られている。この場合、分散配置された 1:1 の LAN 間の接続の場合は、1本の専用線で済むことになるが、M:N 構成の場合は、相互間を接続する為に $M \times N$ 本の専用線が必要となる。従って、データ通信システムの規模が大きくなるに伴って飛躍的に専用線の本数が増加し、コストアップとなる問題がある。

【0003】

そこで、最近のインターネットの普及により、LAN間をインターネットを介して接続して、相互間でデータ通信を行うシステムが実用化されている。その場合、LANとインターネットとの間にファイアウォールを接続して、LANのセキュリティを確保する構成が一般的である。

【0004】

例えば、図9に示すように、インターネット101に対して、ファイアウォール102、103を介して、それぞれ企業内LAN104、105を接続し、企業内LAN104、105は複数のコンピュータ106A、106B、107A、107を接続した構成が知られている。このファイアウォール102、103により、企業内LANに対する不正なアクセスを阻止することができる。

10

【0005】

【発明が解決しようとする課題】

図9に示す従来例に於いては、インターネット101を介して遠隔地の企業内LAN102、103間を接続して、多数の専用線を用いることなく、データ通信を行うことができる。しかし、企業内LAN102、103とインターネット101との間にファイアウォール102、103を設けて、企業内LAN102、103のセキュリティの向上を図ることにより、ファイアウォール102、103は、特定ポートによる接続のみを許容するものであるから、任意のアプリケーションによる接続を阻止することになる。

【0006】

例えば、企業内LAN102のコンピュータ106A、106B間及び企業内LAN103のコンピュータ107A、107B間は、それぞれ同一のLANに接続されているから、任意のアプリケーションによるデータ通信が可能であるが、ファイアウォール102、103を介して接続されたコンピュータ間では、任意のアプリケーションによるデータ通信は不可能となる。そこで、ファイアウォール102、103の特定ポートのオープンや認証機能等の設定変更又はアプリケーションの改造等が必要であった。従って、通信相手先IPやアプリケーションが増える毎に、ファイアウォール102、103の設定変更作業やアプリケーションの改造作業が発生する問題があり、又ポートのオープンによるセキュリティの問題が生じる。

20

【0007】

又イントラネット用のアプリケーションは、そのままインターネット用として適用することができないものであるから、イントラネット用のアプリケーションと、インターネット用のアプリケーションとの二重開発を行わなければならない問題がある。

30

【0008】

又ファイアウォールを介してクライアントとサーバとの間で通信を行う場合に、ファイアウォール等を中継サーバとし、この中継サーバに中継プログラムを実装し、テーブルを参照してクライアントからの通信可能な中継プログラムを選択することが提案されている（例えば、特開平10-126440号公報参照）。しかし、分散配置された企業内LAN等に於いては、ファイアウォール毎に、ネットワーク管理者が異なる場合が一般的である。従って、一元管理ができないことから、運用管理上実現が困難である。

40

【0009】

又アプリケーション自体にファイアウォールを透過させる中継プログラムを実装することが提案されている（例えば、特開2000-115157号公報参照）。しかし、このような構成に於いては、アプリケーションを改造しなければならない問題がある。

【0010】

又VPN（Virtual Private Network：私設仮想網）サービスを適用してデータ通信を行うこともできるが、この場合のデータ通信手段は標準化されていないので、マルチベンダー相互間接続が困難である。

【0011】

又ファイアウォールがHTTP（Hypertext Transfer Protocol）

50

1) によるデータ転送を拒否する場合に、クライアントからのHTTP要求を、中継サーバによりSMTP (Simple Mail Transfer Protocol) に変換してネットワークに送出し、ネットワークを介してサーバ側の中継サーバによりSMTPからHTTPに変換してサーバに転送し、サーバからのHTTP応答を中継サーバによりSMTPに変換してネットワークに送出し、ネットワークを介してクライアント側の中継サーバによりSMTPからHTTPに変換して転送することが提案されている (例えば、特開2001-197125号公報参照)。

【0012】

このようなシステムを送信元イントラネットと送信先イントラネットとの間のデータ通信に適用した場合、データ送信元のコンピュータは、送信先イントラネットのSMTPサーバ↑ファイアウォール↑インターネット↑ファイアウォール↑SMTPサーバの経路で、応答を受信して送達確認を行うことにより、次のデータを送信することになる。その場合、送信先イントラネットが高速回線によって構築されているとは限らず、伝送遅延が大きいと、リアルタイムでデータ通信を行うことが困難となる問題がある。

【0013】

本発明は、前述の従来の問題点を解決するもので、インターネットやファイアウォールを介して接続されていることを意識せずに、TCP (Transmission Control Protocol) 接続によりデータ通信を可能とすることを目的とする。

【0014】

【課題を解決するための手段】

本発明のデータ通信システムは、図1を参照して説明すると、ファイアウォール2、3を介してインターネット1にそれぞれ接続したコンピュータ6A、6B、7A、7Bや企業内LAN4、5等を含む通信装置間でデータ通信を行うデータ通信システムであって、コンピュータ6A、6B、7A、7B等の通信装置とファイアウォール2、3との間に、送信元の通信装置からのデータを、ファイアウォール2、3を透過可能な形式のパケットに変換して送出し、ファイアウォール2、3を介して受信したパケットを送信先の通信装置へのデータに復元するプロトコル変換装置8、9を設け、送信元の通信装置を接続したプロトコル変換装置と送信先の通信装置を接続したプロトコル変換装置との間を、ファイアウォール2、3とインターネット1とを介して中継接続する中継サーバ10を設けた構成とする。

【0015】

又プロトコル変換装置8、9は、送信先の通信装置のアドレスと中継サーバのアドレスとを対応させたルーティングテーブルと、送信元の通信装置からのデータを、ファイアウォールを透過可能な形式のパケットにラッピングするプロトコル変換部と、このプロトコル変換部により変換したパケットを一時格納する送信バッファと、中継サーバとの間の接続要求及び送信バッファから読出したパケットを中継サーバに送出する送信部と、中継サーバから中継送出されたパケットを受信する受信部と、この受信部により受信したパケットを送信先の通信装置に送出するデータに変換するプロトコル変換部とを備えている。

【0016】

又中継サーバ10は、インターネット1を介してプロトコル変換装置8、9との間のコネクションを形成して、送信元側のプロトコル変換装置により変換したパケットを受信する処理部と、この処理部により受信したパケットを一時格納する送信バッファと、この送信バッファからパケットを読出して送信先側のプロトコル変換装置へ送信する処理部とを含む構成を有するものである。又プロトコル変換装置及び中継サーバは、相互間で伝送するパケットに通番を付加して送信し、このパケットを受信して、通番を抽出し、この通番を付加した応答を送信する構成を備えている。又中継サーバ10は、プロトコル変換装置を登録する登録手段と、この登録手段に登録されたプロトコル変換装置間のみ、ファイアウォールを透過可能な形式のパケットの中継送出を行う構成を備えることができる。

【0017】

【発明の実施の形態】

図 1 は本発明の実施の形態の説明図であり、1 はインターネット、2、3 はファイアウォール、4、5 は企業内 LAN、6 A、6 B、7 A、7 B は通信装置としてのコンピュータ、8、9 はプロトコル変換装置、10 は中継サーバを示す。それぞれ複数のコンピュータ 6 A、6 B、7 A、7 B と企業内 LAN 4、5 との間にプロトコル変換装置 8、9 を接続し、企業内 LAN 4、5 とインターネット 1 との間にファイアウォール 2、3 を接続し、インターネット 1 に中継サーバ 10 を接続した場合のデータ通信システムを示す。

【0018】

なお、中継サーバ 10、ファイアウォール 2、3、プロトコル変換装置 8、9、コンピュータ 6 A、6 B、7 A、7 B を更に多数設けた構成とすることも可能であり、又通信装置として、コンピュータ 6 A、6 B、7 A、7 B を用いた場合を示すが、インターネット 1 を介してデータ通信できる構成であれば、コンピュータ以外の構成を適用することができる。

10

【0019】

又プロトコル変換装置 8、9 は、通信装置としてのコンピュータ 6 A、6 B、7 A、7 B からのデータを、ファイアウォール 2、3 を透過可能な形式に変換するものであり、このファイアウォール 2、3 を透過可能な形式のパケットとして、*h t t p* パケットを用いる場合について示す。又コンピュータ 6 A、6 B、7 A、7 B は *I P* パケットを用いて送受信する場合を示し、従って、プロトコル変換装置 8、9 は、*I P* パケットから *h t t p* パケットに変換してファイアウォール 2、3 側に送出し、ファイアウォール 2、3 を介して受信した *h t t p* パケットを *I P* パケットに変換して、コンピュータ 6 A、6 B、7 A、7 B に送出する構成を有するものである。

20

【0020】

又中継サーバ 10 は、インターネット 1 に接続し、企業内 LAN 4、5 間でインターネット 1 を介してデータ通信を行う場合に、プロトコル変換装置 8、9 との間でコネクションを形成し、ファイアウォール 2、3 を透過可能な形式の *h t t p* パケットを中継送出する構成を有するものである。即ち、プロトコル変換装置 8、9 と中継サーバ 10 との間に *h t t p* コネクションを形成して、*h t t p* パケットの中継伝送を行うことにより、コンピュータ 6 A、6 B 側とコンピュータ 7 A、7 B 側との間で、*T C P / I P (T r a n s m i S S i o n C o n t r o l P r o t o c o l / I n t e r n e t P r o t o c o l)* コネクションを形成して、データ通信を行うことができる。

30

【0021】

従って、アプリケーションの改造や、ファイアウォール 2、3 の設定変更を必要としないものとなる。又中継サーバを介してプロトコル変換装置 8、9 間のデータ通信を行い、それぞれにルーティング機能を持たせることにより、専用線接続を必要とすることなく、M : N 間のデータ通信が可能となる。

【0022】

図 2 はプロトコル変換装置 8、9 と中継サーバ 10 との間で送受信するパケットのフォーマットを示し、(a) は送信要求パケット、(b) は送信受付完了通知パケット、(c) は受信要求通知パケットを示す。各パケットは、ファイアウォール 2、3 を透過可能な形式としての *h t t p* パケットとしたもので、*h t t p* ヘッダと、送信、完了通知、受信を示す送受信区分の識別子と、パケット通番とを含むものである。

40

【0023】

又図 2 の (a) に示す送信要求パケットは、送信元コンピュータからの *I P* パケットを、プロトコル変換装置 8、9 に於いてプロトコル変換、即ち、*h t t p* ラッピングを行ったフォーマットを示し、前述のように、*h t t p* ヘッダと、送受信区分の識別子と、パケット通番との次に、プロトコル変換装置 8、9 を一意に識別できる発行元装置 *I D* を付加し、次に、送信先装置 *I D*、*I P* パケット長、暗号化された *I P* パケットを組として、任意数組を順次付加して、*h t t p* パケットを構成する。なお、*I P* データをセキュリティ向上の為に暗号化した場合を示し、プロトコル変換装置 8、9 に於いて暗号化、復号化することができるものであるが、平文データとして送受信することも可能である。

50

【0024】

又図2の(b)の送信受付完了通知パケットは、プロトコル変換装置8, 9からの図2の(a)に示す送信要求パケットに対する応答として、送信要求パケットのパケット通番を送達確認の為に挿入して応答するん七七Pパケットである。又図2の(c)の受信要求通知パケットは、プロトコル変換装置8, 9が中継サーバ10へコネクション要求時に送信するん七七Pパケットであり、最新の受信パケットのパケット通番と自プロトコル変換装置の装置IDとを付加する。

【0025】

図3は本発明の実施の形態の各部の説明図であり、図1と同一符号は同一部分を示し、コンピュータ6, 7間をプロトコル変換装置8, 9とファイアウォール2, 3とインターネットに接続した中継サーバ10とを介してデータ通信を行う場合の各部を構成を示す。又ファイアウォール2, 3と、プロトコル変換装置8, 9と、コンピュータ6, 7とを含めて企業内ネットワークとし、又中継サーバ10と、プロトコル変換装置8, 9との間にん七七Pコネクションを形成し、送信先コンピュータと送信元コンピュータとの間でTCP/IPコネクションを形成して、ファイアウォール2, 3とインターネットとを介してデータ通信を行うものである。

【0026】

コンピュータ6, 7とファイアウォール2, 3との間に接続したプロトコル変換装置8, 9は、IP受信部11, 21と、IP送信部17, 27と、プロトコル変換部12, 22, 16, 26と、ん七七Pパケットを送信するん七七P送信部13, 23と、ん七七Pパケットを受信するん七七P受信部15, 25と、ルーティングテーブル14, 24と、MAC(Media Access Control)テーブル18, 28を含む構成を有するものである。

【0027】

又中継サーバ10は、ん七七P処理部31, 32, 34, 36と、送信バッファを含む送受信処理部33, 36とを有し、図1に示すように、インターネット1に接続されている。なお、ん七七P送信部13, 23は、中継サーバ10に対して送信する送信部、ん七七P受信部15, 25は、中継サーバ10からの受信部である。又中継サーバ10のん七七P処理部31, 34は、プロトコル変換装置からのパケットを受信する処理部、ん七七P処理部32, 35は、プロトコル変換装置へ送信する処理部である。

【0028】

プロトコル変換装置8, 9のIP受信部11, 21は、コンピュータ6, 7からのIPパケットを受信すると、プロトコル変換部12, 22に転送する。プロトコル変換部12, 22は、ルーティングテーブル14, 24を参照して、中継サーバ10のIPアドレスを求め、IPパケットをん七七Pにラッピングし、ん七七P送信部13, 23からファイアウォール2を介してインターネットに接続した中継サーバ10にん七七Pパケットを送信する。

【0029】

中継サーバ10は、ん七七P処理部31, 34により受信したん七七Pパケットを送受信処理部33, 36を介してん七七P処理部32, 35に転送し、ん七七Pパケットをファイアウォール2, 3を介してプロトコル変換装置8, 9に送信する。プロトコル変換装置8, 9のん七七P受信部15, 25は、中継サーバ10からのん七七Pパケットを受信すると、プロトコル変換部16, 26に転送し、プロトコル変換部16, 26は、アンラッピングによりん七七PパケットからIPパケットを取り出し、MACテーブル18, 28を参照して、IP送信部17, 27からコンピュータ6, 7へIPパケットを送信する。

【0030】

図4は本発明の実施の形態のプロトコル変換装置の説明図であり、図3に於けるコンピュータ6に接続したプロトコル変換装置8を示すもので、コンピュータ7に接続したプロトコル変換装置9も同一の構成を有するものである。なお、中継サーバ10との間のファイアウォール2は図示を省略している。

10

20

30

40

50

【0031】

プロトコル変換装置8は、プロトコル変換して中継サーバ10側へ送信する送信部としての機能と、中継サーバ10側から受信してプロトコル変換する受信部としての機能とを有し、図4に於いては、上側が送信部、下側が受信部を構成している。又図4に於いて、11はIP受信部、12はプロトコル変換部、13はhттP送信部、14はルーティングテーブル、15はhттP受信部、16はプロトコル変換部、17はIP送信部、18はMACテーブル、41は送信通番テーブル、42は送信バッファ、43は受信通番テーブルを示す。

【0032】

IP受信部11は、コンピュータ6からのIPパケットを受信すると、プロトコル変換部12に転送する。このプロトコル変換部12は、IPパケットをhттPラッピングする機能を有し、ルーティングテーブル14と送信通番テーブル41とを参照して、IPパケットの送信先コンピュータに対応する中継サーバ及び送信先装置IDを決定し、パケット通番を付加して、図2の(a)に示す送信要求パケットを形成し、送信バッファ42に転送し、且つhттP送信部13に、送信バッファ42に格納したことを示すバッファ更新通知を行う。

【0033】

ルーティングテーブル14は、例えば、図5の(A)に示すように、送信先IPアドレスに対応したプロトコル変換装置の装置IDと、中継サーバIPアドレスとを含むものである。従って、IPパケットの送信先のIPアドレスを基に、送信要求パケットに付加する送信先装置IDと、hттPパケットを送信する中継サーバとを決定することができる。即ち、インターネットに接続された複数の中継サーバについて、送信先のIPアドレスに対応した中継サーバを指定することができる。又送信通番テーブル41は、送信要求パケットのパケット通番を管理するテーブルであり、送信する中継サーバ毎に一意となるパケット通番を送信要求パケットに付加するものである。

【0034】

又送信バッファ42は、送信先中継サーバ毎にバッファリングする構成を有し、又同一中継サーバ向けの未送信要求パケットが存在する場合、プロトコル変換部12は、その送信要求パケットにIPパケットを追加する。その場合、図2の(a)に示すように、複数組のIPパケットを含む送信要求パケットとして、送信バッファ42に格納されることになる。そして、hттP送信部13にバッファ更新通知を行い、hттP送信部13は、中継サーバ10にhттP接続要求を行い、hттPコネクション確立後、送信バッファ42から送信要求パケットを読出して中継サーバ10に送信する。

【0035】

中継サーバ10は、送信要求パケットを受信すると、送信要求パケットのパケット通番を抽出し、このパケット通番を付加して、図2の(b)に示す送信受付完了通知パケットを受付応答として送出する。この送信受付完了通知パケットをhттP送信部13が受信確認すると、その送信受付完了通知パケットに付加された送信要求時のパケット通番を識別し、このパケット通番を含むそれ以前のパケット通番のhттPパケットは送達確認ができたものであるから、送信バッファ42から送信完了として削除する。又この送達確認が得られる前に送信バッファ42にプロトコル変換部12の処理により格納したパケットは、送達確認が得られ後、hттPコネクションを形成し、一括して送信先中継サーバに送出する制御を行うこともできる。

【0036】

又hттP受信部15は、予め定義している接続可能の中継サーバ10に対してhттP接続要求を行い、hттPコネクション確立後、図2の(c)に示す受信要求通知パケットを中継サーバ10に送信し、中継サーバ10から、図2の(a)に示すフォーマットの送信要求パケットを応答として受信すると、プロトコル変換部16に転送し、受信通番テーブル43により、送信要求パケットのパケット通番を保持し、次の受信要求時に、最新の受信したパケット通番を受信要求通知パケットに格納して送信する。中継サーバ10

10

20

30

40

50

は、この受信要求通知パケットに付加された最新に受信したパケット通番を抽出して送達確認を行うことができる。

【0037】

又プロトコル変換部16は、h t t p 受信部15から転送された送信要求パケットについて、h t t p アンラッピングによりIPパケットに復元し、M A C テーブル18を参照して、送信先IPアドレスに対するM A C アドレスを付与して、IP送信部17に転送し、IP送信部17からコンピュータ6に送信する。M A C テーブル18は、例えば、図5の(B)に示すように、送信先IPアドレスに対応する送信先M A C アドレスを格納している。

【0038】

図6は本発明の実施の形態の中継サーバの説明図であり、図3に於けるプロトコル変換装置8、9間の中継サーバ10のh t t p 処理部31、32と、送受信処理部33とに対応する要部を示し、送受信判断部51、54と、通番管理テーブル52と、送信バッファ53とにより、送受信処理部33を構成している。

【0039】

h t t p 処理部31は、プロトコル変換装置8からのh t t p 接続要求により、h t t p コネクションを確立し、h t t p ポートによってプロトコル変換装置8からの送信要求パケットを受信すると、送受信判断部51に転送する。又送受信判断部51から依頼された送信受付完了通知パケットをプロトコル変換装置8へ送信し、又h t t p 切断を通知する機能を有する。h t t p 処理部32も同様に、プロトコル変換装置9からのh t t p 接続要求によりh t t p コネクションを確立し、h t t p ポートによってプロトコル変換装置9からの送信要求通知パケットを受信すると、送受信判断部54に転送し、又送受信判断部54からの送信要求パケットをプロトコル変換装置9に送信し、又h t t p 切断を通知する機能を有するものである。

【0040】

又送受信判断部51は、h t t p 処理部31から転送されたパケットの内容を解析し、送信要求か受信要求かを判断し、送信要求パケットの場合、送信先プロトコル変換装置毎の送信バッファ53に格納する。この場合、複数組のIPパケットを含む場合に、IPパケット毎に分解し、送信先装置ID毎に送信バッファ53に格納することができる。又通番管理テーブル52により、送信先プロトコル変換装置毎に、送信要求パケットに付加されたパケット通番を管理し、送信受付完了通知を送出する場合に、このパケット通番を用いるものである。

【0041】

送信要求パケットを受信して送信バッファに格納すると、送信受付完了通知パケットを送信するようにh t t p 処理部に通知し、図2の(b)に示す送信要求時パケット通番を付加した送信受付完了通知パケットをプロトコル変換装置8に送信する。従って、プロトコル変換装置8は、この送信受付完了通知パケットを受信して、パケット通番によって送達確認を行い、このパケット通番の送信要求パケットが送信バッファ42に残っていると、送信完了パケットであるから、これを削除し、又送信バッファ42に未送信のデータが残存していると、h t t p 送信部18から送信することになる。

【0042】

又送受信判断部54は、h t t p 処理部32から転送されたパケットの内容を解析し、受信要求通知パケットの場合、送信バッファ53の送信先プロトコル変換装置対応の領域にパケットが存在しているか否かを判断し、存在していない場合は、その領域を監視し、パケットが格納されていると、それを読み出して送信要求パケットを組立て、h t t p 処理部32に転送し、このh t t p 処理部32からプロトコル変換装置9に対して送信要求パケットを送信する。

【0043】

この送信要求パケットに対して、プロトコル変換装置9からの受信要求通知パケットを受信すると、それに付加されている最新に受信したパケット通番と同一のパケット通番の

10

20

30

40

50

ケットは送信完了と判断して、送信バッファ53から削除し、未送信のケットが残っている場合は、送信バッファ53から読出して、h77P処理部32からプロトコル変換装置9に送信し、総ての送信が終了すると、h77P切断とする。この送信バッファ53に於いても、送信先のプロトコル変換装置からの送達確認が得られる前に、送信元のプロトコル変換装置からの送信要求ケットを格納した時は、送達確認が得られた後、h77Pコネクションを形成して、一括して送信先のプロトコル変換装置に送信することができる。

【0044】

図7はコンピュータ6からプロトコル変換装置8を介して中継サーバ10に送信する場合のシーケンスを示し、図3、図4、図6を参照して説明する。送信元のコンピュータ6から送信先のコンピュータ7に対してIPケットを送信すると、プロトコル変換装置8に於いては、IP受信部11により受信してプロトコル変換部12に転送する。プロトコル変換部12は、ルーティングテーブル14を参照して中継サーバのIPアドレスを求め、h77PラッピングによりIPケットをh77Pケットに変換し、又ケット通番を付与して送信バッファ42に格納し、h77P送信部13に対してバッファ更新通知を送出する。

10

【0045】

h77P送信部13は、中継サーバ10に対してh77P接続要求を送出してh77Pコネクションを確立し、送信要求ケットを送信バッファ42から読出して送信する。中継サーバ10のh77P処理部31は、送信要求ケットを送受信判断部51に転送し、送受信判断部51は、送信要求ケットを送信バッファ53に格納し、ケット通番を付加した送信受付完了ケットをh77P送信部31に転送し、h77P送信部31からプロトコル変換装置8に送信し、h77P切断を行う。プロトコル変換装置8のh77P送信部13は、送信受付完了ケットに付加された通番を基に送信完了したケットを送信バッファ42から削除する。

20

【0046】

図8は中継サーバ10からプロトコル変換装置9を介して送信先のコンピュータ7に送信する場合のシーケンスを示し、プロトコル変換装置9のh77P受信部25からh77P接続要求を送出して中継サーバ10との間のh77Pコネクションを確立し、受信要求通知ケットを送信する。

30

【0047】

中継サーバ10のh77P処理部32は、受信要求通知ケットを送受信判断部54に転送する。この送受信判断部54は、送信バッファ53から未送信ケットを抽出し、送信要求ケットとしてh77P処理部32に転送する。h77P処理部32は、この送信要求ケットをプロトコル変換装置9に送信してh77P切断を行う。

【0048】

プロトコル変換装置9のh77P受信部25に於いて送信要求ケットを受信すると、プロトコル変換部26に転送し、h77PアンラッピングによりIPケットに分離し、IP送信部27からコンピュータ7にIPケットを送信する。前述の動作を繰り返すことにより、中継サーバ10からコンピュータ7に対してh77PラッピングによるIPケットを送信することができる。

40

【0049】

又ファイアウォール2、3とプロトコル変換装置8、9との間に、プロキシサーバが存在するシステムの場合、プロトコル変換装置8、9の受信処理に於いて、受信要求通知ケットを送出するコネクションがタイムアウトにより切断される可能性がある。しかし、プロトコル変換装置8、9からの受信要求通知ケットの送出手は、リトライ動作を行うことを可能としているもので、そのリトライ動作による受信要求通知ケットの送出手によって形成したコネクションにより、プロトコル変換装置8、9は、中継サーバ10からの送信要求ケットを受信することができる。

【0050】

50

又中継サーバ１０に、登録テーブル等の登録手段を設け、この登録手段に、通信可能のプロトコル変換装置を送信先装置ＩＤとして登録し、送受信判断部５１、５４は、送信先装置ＩＤを識別できるから、登録手段を参照して、登録された送信先装置ＩＤを有する送信要求パケットの中継伝送を可能とすることができる。それにより、通信できる相手プロトコル変換装置を制限して、セキュリティの向上を図ることができる。

【００５１】

本発明は、前述の各実施の形態のみに限定されるものではなく、種々付加変更することが可能である。例えば、中継サーバ１０の送信バッファ５３に送信要求パケットが格納された時に、送受信判断部５４の判断処理により、送信先のプロトコル変換装置に対するコネクションを設定し、そのプロトコル変換装置からの応答に従って、送信要求パケットを送出する制御構成とすることも可能である。又送信バッファ４２、５３に一時格納された送信要求パケットを読み出して送信する毎に、コネクションを切断することができる。

【００５２】

（付記１）ファイアウォールを介してインターネットにそれぞれ接続した通信装置間でデータ通信を行うデータ通信システムに於いて、前記通信装置と前記ファイアウォールとの間に、送信元の通信装置からのデータを前記ファイアウォールを透過可能な形式のパケットに変換して送出し、前記ファイアウォールを介して受信した前記パケットを送信先の通信装置へのデータに復元するプロトコル変換装置を設け、送信元の通信装置を接続したプロトコル変換装置と送信先の通信装置を接続したプロトコル変換装置との間を前記ファイアウォールと前記インターネットとを介して中継接続する中継サーバを設けたことを特徴とするデータ通信システム。

（付記２）前記プロトコル変換装置は、送信先の通信装置のアドレスと前記中継サーバのアドレスとを対応させたルーティングテーブルと、送信元の通信装置からのデータを前記ファイアウォールを透過可能な形式のパケットにラッピングするプロトコル変換部と、該プロトコル変換部により変換したパケットを一時格納する送信バッファと、前記中継サーバとの間の接続要求及び前記送信バッファから読み出したパケットを前記中継サーバに送出する送信部と、前記中継サーバから中継送出されたパケットを受信する受信部と、該受信部により受信したパケットを送信先の通信装置に送出するデータに変換するプロトコル変換部とを備えたことを特徴とする付記１記載のデータ通信システム。

【００５３】

（付記３）前記プロトコル変換装置の前記送信バッファは、前記ルーティングテーブルを参照して求めた送信先中継サーバ対応に送信要求パケットを格納する構成を有することを特徴とする付記２記載のデータ通信システム。

（付記４）前記中継サーバは、前記インターネットを介して前記プロトコル変換装置との間のコネクションを形成して、送信元側の前記プロトコル変換装置により変換したパケットを受信する処理部と、該処理部により受信したパケットを一時格納する送信バッファと、該送信バッファからパケットを読み出して送信先側の前記プロトコル変換装置へ送信する処理部とを含む構成を有することを特徴とする付記１記載のデータ通信システム。

（付記５）前記中継サーバの前記送信バッファは、前記処理部の制御に従って送信先のプロトコル変換装置対応に送信要求パケットを格納する構成を有することを特徴とする付記４記載のデータ通信システム。

【００５４】

（付記６）前記プロトコル変換装置及び前記中継サーバは、相互間で伝送するパケットに通番を付加して送信し、該パケットを受信して前記通番を抽出し、該通番を付加した応答を送信する構成を備えたことを特徴とする付記１乃至３の何れかに記載のデータ通信システム。

（付記７）前記中継サーバは、前記プロトコル変換装置を登録手段と、該登録手段に登録されたプロトコル変換装置間のみ前記ファイアウォールを透過可能な形式のパケットの中継伝送を行う構成を備えたことを特徴とする付記１乃至４の何れかに記載のデータ通信システム。

10

20

30

40

50

【 0 0 5 5 】

【 発 明 の 効 果 】

以上説明したように、本発明は、コンピュータ 6 A、6 B、7 A、7 B等の通信装置とファイアウォール 2、3との間にプロトコル変換装置 8、9を設け、又インターネット 1に中継サーバ 10を設けて、プロトコル変換装置 8、9によりファイアウォール 2、3を透過可能な TCP パケット等の形式に変換し、中継サーバ 10とプロトコル変換装置 8、9との間にコネクションを形成して、送信元のプロトコル変換装置と送信先のプロトコル変換装置との間で、ファイアウォール 2、3を透過させて、通信装置間でデータ通信を行うものであり、従って、インターネット 1を介して TCP/IP による通信を行う場合に、プロトコル変換装置 8、9と中継サーバ 10とに於けるルーティング処理により、送信元の通信装置と送信先の通信装置との間にファイアウォール 2、3が介在していても、ファイアウォール 2、3の設定変更を行うことなく、データ通信を行うことができ、且つ専用線による M:N 接続の場合と同様に、複数の企業内 LAN 間でインターネット 1を介してデータ通信を行うことができる。

10

【 0 0 5 6 】

又プロトコル変換装置 8、9と中継サーバ 10とのそれぞれの間で送達確認を行うことにより、送信元の通信装置と送信先の通信装置との間でデータ通信を行うことができるもので、例えば、インターネットを介して接続したイントラネット間でデータ通信を行う場合の送達確認を行う場合、従来例の SMTP により送達確認を行う構成に比較して、伝送遅延による問題がなくなる。又イントラネット用の既存のアプリケーションを、セキュリティを確保した上で、そのままインターネット用としてリアルタイム通信を可能とすることから、イントラネット用のアプリケーションとインターネット用のアプリケーションとの二重開発の必要がなくなる利点がある。

20

【 図 面 の 簡 単 な 説 明 】

【 図 1 】 本発明の実施の形態の説明図である。

【 図 2 】 パケットフォーマットの説明図である。

【 図 3 】 本発明の実施の形態の各部の説明図である。

【 図 4 】 本発明の実施の形態のプロトコル変換装置の説明図である。

【 図 5 】 ルーティングテーブル及び MAC テーブルの説明図である。

【 図 6 】 本発明の実施の形態の中継サーバの説明図である。

30

【 図 7 】 本発明の実施の形態の送信処理シーケンス説明図である。

【 図 8 】 本発明の実施の形態の受信処理シーケンス説明図である。

【 図 9 】 従来のデータ通信システムの説明図である。

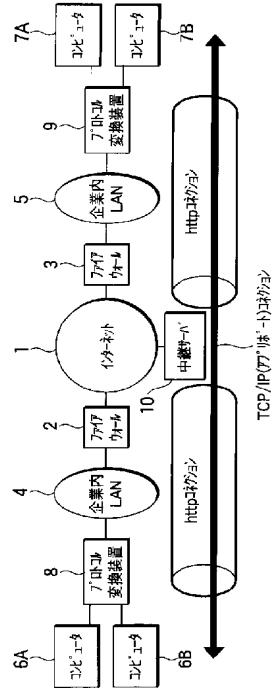
【 符 号 の 説 明 】

- 1 インターネット
- 2、3 ファイアウォール
- 4、5 企業内 LAN
- 6 A、6 B、7 A、7 B コンピュータ
- 8、9 プロトコル変換装置
- 10 中継サーバ

40

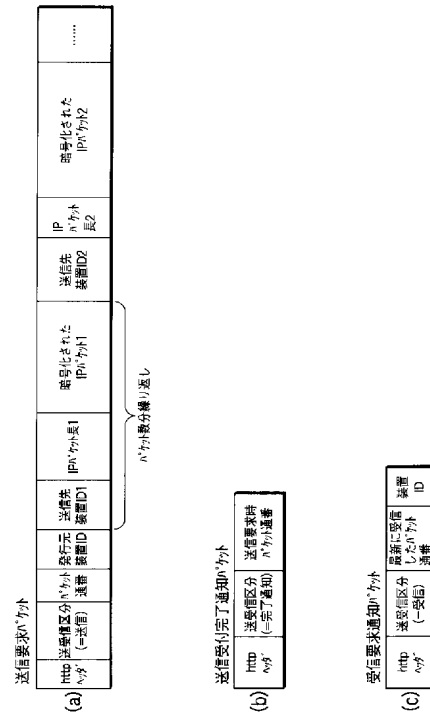
【図 1】

本発明の実施の形態の説明図



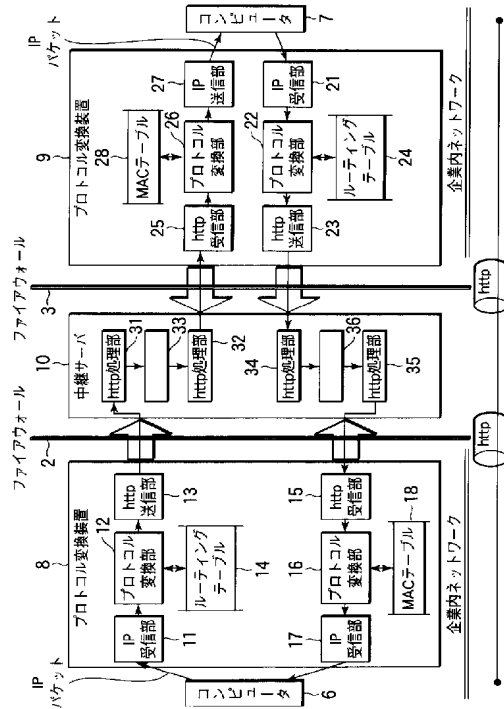
【図 2】

パケットフォーマットの説明図



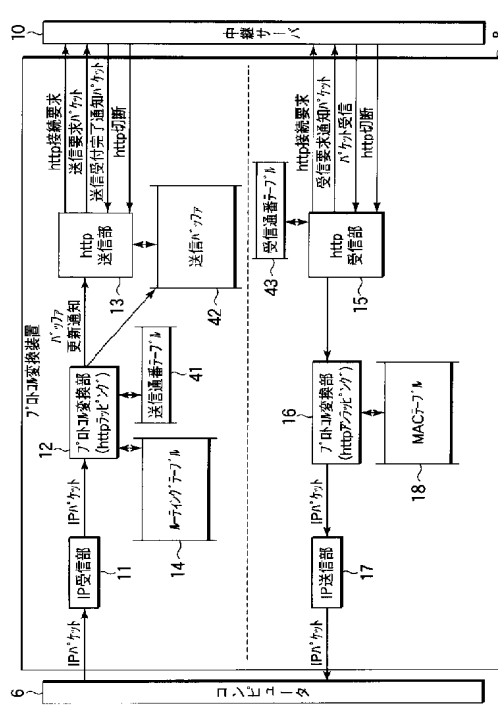
【図 3】

本発明の実施の形態の各部の説明図



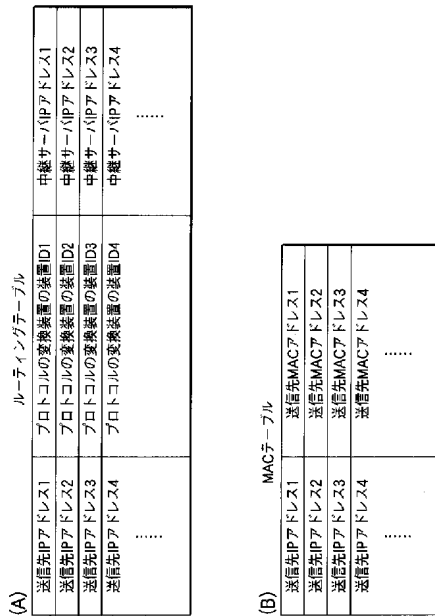
【図 4】

本発明の実施の形態のプロトコル変換装置の説明図



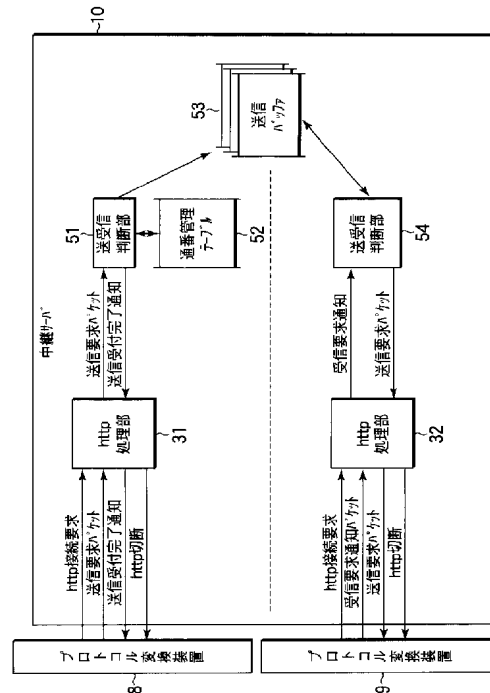
【図 5】

ルーティングテーブル及びMACテーブルの説明図



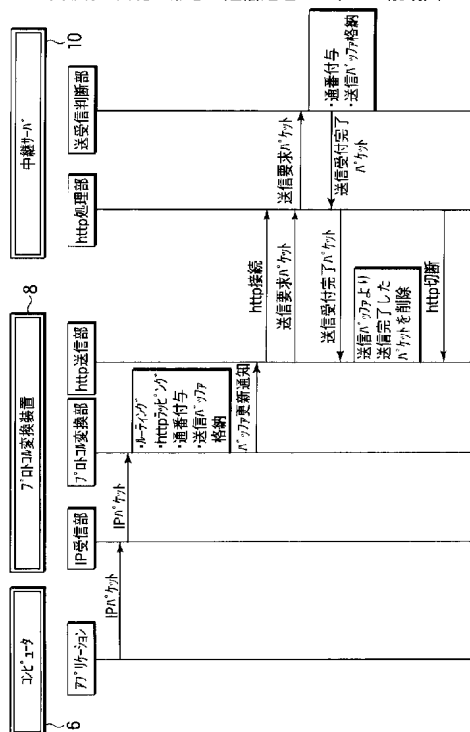
【図 6】

本発明の実施の形態の中継サーバの説明図



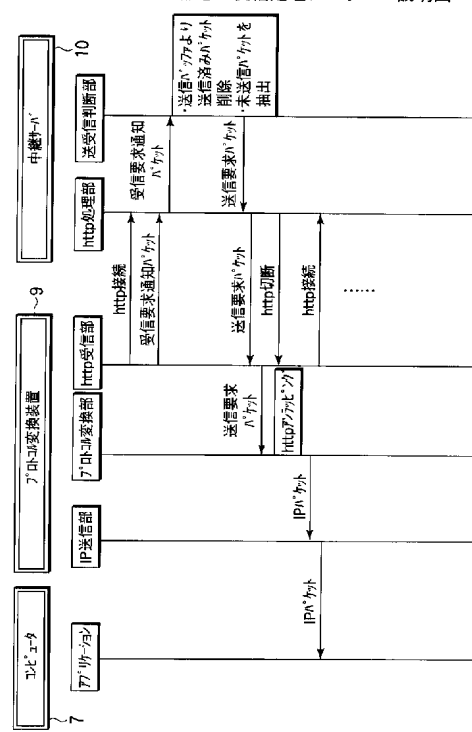
【図 7】

本発明の実施の形態の送信処理シーケンス説明図



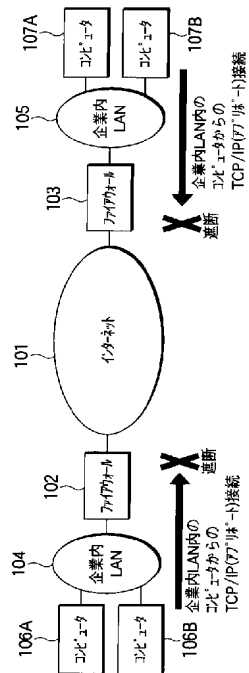
【図 8】

本発明の実施の形態の受信処理シーケンス説明図



【図 9】

従来のデータ通信システムの説明図



フロントページの続き

(72)発明者 林田 孝

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(72)発明者 貝塚 智憲

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(72)発明者 下山 元章

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

(72)発明者 佐藤 寛子

神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

Fターム(参考) 5B089 KA17 KB03 KB13

5K030 GA08 HA08 HB18 HD09 KA04 KX24 LB15 LD19

5K034 AA18 DD01 EE10 FF01 FF11 HH61